

# Intel® vPro™ Technology Use Case Reference Design

RealVNC VNC\* Viewer Plus with Microsoft\*  
System Center Configuration Manager

---

Revision 1.0  
January, 2011  
Document ID: 1042

# Revision History

Revision	Revision History	Date
1.0	Initial release.	January, 2011

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

EXCLUSION OF OTHER WARRANTIES. THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY KIND, INCLUDING WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. Intel does not warrant or assume responsibility for the accuracy or completeness of any information, text, graphics, links or other items contained within the Software.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The Intel® Active Management Technology may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web Site.

Intel® Active Management Technology requires the computer system to have an Intel(R) AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see [www.intel.com/technology/platform-technology/intel-amt/](http://www.intel.com/technology/platform-technology/intel-amt/)

Throughout this document Intel ME refers to Intel® Management Engine and Intel® AMT refers to Intel® Active Management Technology.

Intel , the Intel logo, Intel® AMT, and Intel® vPro™ are trademarks or registered trademarks of Intel Corporation in the United States and other countries.

\*Other names and brands may be claimed as the property of others.

Copyright © 2011 Intel Corporation. All rights reserved.

# Contents

---

<b>1</b>	<b>Preface .....</b>	<b>5</b>
1.1	Document Scope .....	5
1.2	Intended Audience .....	5
1.3	Related Documentation .....	5
<b>2</b>	<b>Introduction .....</b>	<b>6</b>
2.1	What You Need .....	7
2.2	Process Overview .....	7
<b>3</b>	<b>Help Desk Level Configuration.....</b>	<b>9</b>
3.1	KVM Remote Control Configuration Tool .....	9
3.2	Automating the Configuration.....	11
3.3	Alternative Configurations.....	13
3.3.1	Specify the Admin Credentials .....	13
3.3.2	Using a standard VNC viewer .....	14
3.3.3	Disable User Consent .....	14
<b>4</b>	<b>Using RealVNC VNC* Viewer Plus .....</b>	<b>15</b>
4.1	Configuring Viewer Plus .....	15
4.2	Establishing a KVM Remote Control Session .....	15
<b>Figures</b>		
Figure 1:	The KVM Remote Control Configuration Tool Screen.....	10
Figure 2:	Successful Output of KVMon.bat .....	11
Figure 3:	Query Rules Property Button.....	12
Figure 4:	New Criteria Button .....	12
Figure 5:	Setting User Consent to Off in VNC Viewer Plus .....	14



# 1 Preface

---

Although Microsoft\* System Center Configuration Manager (ConfigMgr) has support for Intel® Active Management Technology (Intel® AMT), Microsoft has not yet (as of this writing) added support for Intel AMT's KVM Remote Control feature. This document provides required steps to use RealVNC's VNC\* Viewer Plus for KVM Remote Control of Intel® vPro™ technology enabled systems that have been set up and configured using ConfigMgr.

## 1.1 Document Scope

This document describes how to use RealVNC's VNC Viewer Plus with Intel AMT 6 and above in a server-TLS, Kerberos environment. It assumes Intel AMT setup and configuration is handled by ConfigMgr. This document does NOT cover using ConfigMgr or configuring Intel AMT with ConfigMgr. Rather, it is assumed the reader is familiar with both ConfigMgr and Intel AMT.

## 1.2 Intended Audience

This document is intended for Information Technology (IT) professionals who are interested in taking advantage of Intel AMT at their help desk or who are interested in experimenting with and learning about KVM Remote Control.

## 1.3 Related Documentation

The following documents may be useful in further understanding Intel vPro technology and its features and RealVNC's VNC Viewer Plus.

- RealVNC VNC\* Viewer Plus user guide; see chapter 2 for breakdown into six easy steps.:  
<http://www.realvnc.com/products/viewerplus/1.0/>
- Additional Use Case Reference Designs, including Remote Drive Sharing:  
<http://communities.intel.com/docs/DOC-4080>
- Out-of-Box Configuration for KVM Remote Control:  
<http://communities.intel.com/docs/DOC-4795>
- Help Desk Console for Non-TLS Environments, describes using RealVNC VNC Viewer Plus in a Digest, non-TLS environment with emphasis on help desk tasks.  
<http://communities.intel.com/docs/DOC-4910>
- ConfigMgr references:
  - Extra Intel AMT Configuration with ConfigMgr:  
<http://communities.intel.com/docs/DOC-5215>
  - EZ Help Desk permissions with ConfigMgr:  
<http://communities.intel.com/docs/DOC-4404>
  -

## 2 Introduction

---

It is possible to use various management consoles and tools that support Intel AMT with Intel AMT enabled systems that have been set up and configured by Microsoft System Center Configuration Manager (ConfigMgr). This is especially useful with respect to KVM Remote Control as the current ConfigMgr (as of this writing) does not provide a KVM tool. This document will outline how to use Real VNC Viewer Plus with Intel AMT's that were provisioned with ConfigMgr.

This document covers two possible security configurations. The first, Admin Level, is the simplest. In this configuration anyone who uses KVM Remote Control must have administrative rights to Intel AMT. In the second configuration, called Help Desk Level, users only need Help Desk level permissions to use KVM Remote Control. These two permission levels are discussed in detail in the UCRD document *EZ Helpdesk Permissions with ConfigMgr*, available at the following link:

<http://communities.intel.com/docs/DOC-4404>.

This added security and flexibility is gained by performing some of the KVM Remote Control configuration before Help Desk personnel can use it.

This document recommends trying a test system with Admin Level first. Then, if desired, try Help Desk Level on a test system.

Please note that this UCRD document builds upon other existing UCRD documents. Consequently, many specific steps have been omitted from this document, with references provided to other documents where applicable. In sections where these steps are original or deviate from other UCRD documents, this document will provide specifics.

UCRD Document	Link	Method used in
Out-of-Box Configuration for KVM Remote Control	<a href="http://communities.intel.com/docs/DOC-4795">http://communities.intel.com/docs/DOC-4795</a>	2
Help Desk Console for Non-TLS Environments, describes using RealVNC Viewer Plus in a Digest, non-TLS environment with emphasis on help desk tasks.	<a href="http://communities.intel.com/docs/DOC-4910">http://communities.intel.com/docs/DOC-4910</a>	1, 2
Extra Configuration for Intel AMT with Microsoft ConfigMgr	<a href="http://communities.intel.com/docs/DOC-5215">http://communities.intel.com/docs/DOC-5215</a>	2

EZ Help Desk permissions with Microsoft ConfigMgr	<a href="http://communities.intel.com/docs/DOC-4404">http://communities.intel.com/docs/DOC-4404</a>	2
---	---	---

## 2.1 What You Need

The steps in this document have the following requirements:

ConfigMgr Server	ConfigMgr 2007 Service Pack 1 or 2, configured for use with Intel vPro technology. See the following link: <ul style="list-style-type: none"> <li><a href="http://www.microsoft.com/systemcenter/configurationmanager/en/us/default.aspx">http://www.microsoft.com/systemcenter/configurationmanager/en/us/default.aspx</a></li> </ul> <b>Note:</b> Windows* 2003 with SP2 and SQL Server 2005 were used when writing these instructions. Other OS or SQL versions may have different specific steps. However, the overall process and concepts are the same.
Managed Client with Intel vPro technology	Intel AMT 6.0 or later and supporting the KVM Remote Control feature. Intel AMT 6.0 is setup and configured by ConfigMgr in a Server TLS environment and Kerberos environment.
Console System	Any XP, Windows 7, Windows 2003, or Windows 2008 system that is a domain member may be used. The ConfigMgr Server may be used for this role if desired.  Must be able to log on to this system as a user with AMT Admin permissions and optionally a user with Help Desk Level AMT permissions.
Optional: A user with Help Desk Level Permissions	Only required for Help Desk Level. Follow this document to setup help desk level permissions for an Active Directory group: <a href="http://communities.intel.com/docs/DOC-4404">http://communities.intel.com/docs/DOC-4404</a>

## 2.2 Process Overview

For the Admin level configuration, this process is quite simple. VNC Viewer Plus was designed to handle all KVM Remote Control configuration automatically. As such, you simply connect to Intel AMT and begin using KVM Remote Control. The requirement here is that your user account has admin permissions in Intel AMT. If you wish to use this method, skip ahead to section 4, Using RealVNC VNC\* Viewer Plus, on page 15.

For the Help Desk Level configuration, some pre-work is required. This is because Admin rights are required to enable KVM Remote Control. However, only Help Desk rights are required to use KVM Remote Control. So, a KVM Remote Control configuration tool (such as the one provided here:

<http://communities.intel.com/docs/DOC-4795>) is used to first enable KVM Remote Control.



## NOTE

*Intel AMT has various permission levels called Realms. This document considers “Help Desk Level” to include the General Info, Redirection and the Remote Control realms. To use KVM Remote Control only Redirection is required. Remote Control is required to perform remote reboots (such as rebooting to an IDER disk), which is an essential capability for a help desk user.*

Once a working configuration is established, scripts (provided here: <http://communities.intel.com/docs/DOC-5215>) can be used in conjunction with ConfigMgr to automate this process.

Also note that for the Help Desk Level configuration *only*, a user with Help Desk level permissions must be set up in Intel AMT. See <http://communities.intel.com/docs/DOC-4404> for detailed steps. This document assumes Intel AMT already has such a user configured. For the purpose of this document, the user is name vprodemo\helpdesk.

Please refer to the following RealVNC document describing what a Help Desk (or Standard) User can do:

<http://www.realvnc.com/products/viewerplus/1.1/docs/ag1030244.html>



## 3 Help Desk Level Configuration

---

The sections below describe steps specific to setting up and automating the Help Desk level Configuration.



### NOTE

*This document assumes Intel AMT already has a user configured with Help Desk Level permissions. See <http://communities.intel.com/docs/DOC-4404> for steps.*

### 3.1 KVM Remote Control Configuration Tool

In this step we configure and test KVM Remote Control on a single Intel AMT 6 system to establish a working configuration.

1. Login to the Console as a user with Administrative rights to Intel AMT.
2. Download this UCRD, *Out-of-Box Configuration for KVM Remote Control*:  
<http://communities.intel.com/docs/DOC-4795>
3. Using the instructions in the *Out-of-Box Configuration for KVM Remote Control* UCRD, extract the KVM folder included in that UCRD to **c:\kvm**.



### NOTE

*This tool requires WinRM. Windows 2008 includes WinRM. Windows 2003 does not. If your system does not already have WinRM, follow steps in section 4.2 from the downloaded UCRD document to install it.*

4. Run **c:\kvm\kvm.hta**.
5. If you have not already configured WinRM, click **Configure WinRM** in the top section labeled **Step 1**.

6. In the **Step 2** section, click **Advanced Settings**. The screen should now look similar to Figure 1 below.

The screenshot shows a window titled "KVM Remote Control Configuration". It is divided into two sections: Step 1 and Step 2.

**Step 1**

Click the button below to configure WinRM. This must be done before remotely configuring Intel AMT below. Only needs to be run once per management console.

---

**Step 2**

Enter the information below and click **Enable** to remotely configure Intel AMT for KVM Remote Control on the specified managed client. To reset to the default disabled state, click **Disable**.

FQDN or IP Address:  FQDN or IP Address of your Managed Client

Use TLS:  Use Server TLS to communicate with AMT

Use Kerberos:  User Kerberos to Login to AMT

Use Currently Logged in Credentials:  If set to yes, the username and password below are ignored.

Admin User Name:  Admin User Name for Intel AMT on the Managed Client. **Example for digest:** admin. **Example for Kerberos:** vprodemo.com\itproadmin

Admin Password:  Admin Password for Intel AMT on the Managed Client

New RFB Password:  New Password to be used with KVM Remote Control Sessions. Note: Must be exactly 8 characters and be a strong password.

Enable KVM Only:  If set to yes (1) then KVM will be enabled. However, Port 5900 and RFBPassword settings will not be changed. This is mainly used when a non-admin AMT user will be using a KVM remote control enabled tool such as RealVNC Viewer Plus.

**Figure 1: The KVM Remote Control Configuration Tool Screen**

7. Configure the settings in the **Step 2** section to match those shown in Figure 1 above, then click **Save Settings**.

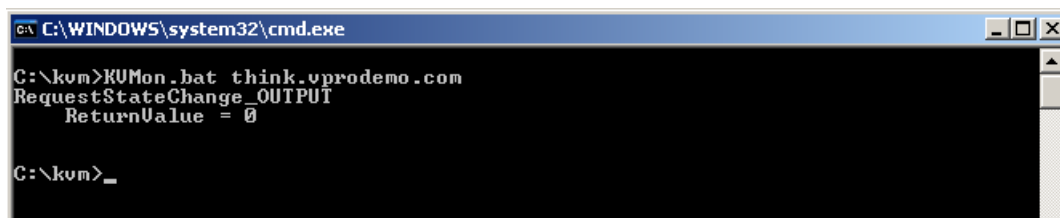


#### NOTE

*There are other possible configurations, though those are not covered in detail. Section 3.3 contains further information on alternative configurations.*

8. Close **kvm.hta**.
9. Open a command prompt as administrator and enter **cd \kvm**.

10. Enter **kvmon.bat** **<FQDN>** where **<FQDN>** is the fully qualified domain name of your Intel AMT 6 enabled client. Figure 2 shows successful output.



```
C:\WINDOWS\system32\cmd.exe

C:\kvmon>KVMon.bat think.oprodemo.com
RequestStateChange_OUTPUT
Return Value = 0

C:\kvmon>_
```

**Figure 2: Successful Output of KVMon.bat**

At this point Intel AMT may be used by a user with help desk level permissions. Log out of the console and log back in as a user with Help Desk Level permissions. Now, try KVM Remote Control to test that everything works. Refer to section 4, Using RealVNC VNC\* Viewer Plus, on page 15 for more information. Once the test is confirmed, continue on to section 3.2 below.

## 3.2 Automating the Configuration

Now that you have a working configuration, you may choose to automate the configuration of all your Intel vPro technology based systems. This process is documented in the UCRD document *Extra Configuration for Intel AMT Using Microsoft ConfigMgr*, available at: <http://communities.intel.com/docs/DOC-5215>. As such this document will provide some pointers, but will not cover all steps.

In the UCRD document referenced above, section 3 covers preparing your extra configuration tool. That process is covered in section 3.1 of this document. Just be sure to keep all files in **c:\kvmon** in the same folder. Your working command line is **c:\kvmon\Kvmon.bat <FQDN>** where **<FQDN>** is the fully qualified domain name of your Intel AMT 6 enabled PC.

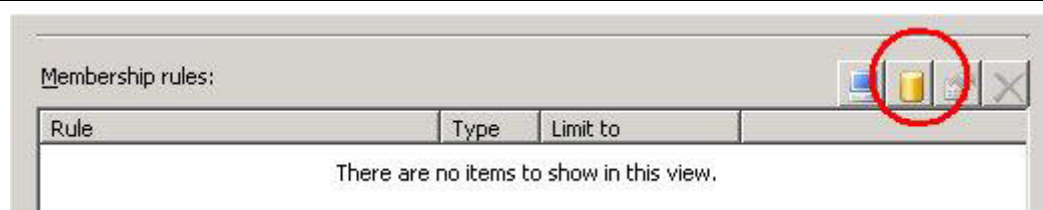
If you choose the Database Trigger method (section 4 of *Extra Configuration for Intel AMT Using Microsoft ConfigMgr*), note that kvmon.bat will be run against all Intel AMT enabled systems, regardless of version. This should not cause a problem, but be aware that any logging will show failures on any Intel AMT enabled system below version 6.0.

If you choose the Configuration Manager Collection method (section 5 of *Extra Configuration for Intel AMT Using Microsoft ConfigMgr*), here are steps to create a ConfigMgr collection to identify KVM capable systems. This can be used for the first collection in section 5.1 of *Extra Configuration for Intel AMT Using Microsoft ConfigMgr*:

The example outlines identifying all KVM capable systems. You may modify the query as desired to suit your needs.

In the ConfigMgr Console, perform the following steps:

1. In the left-hand navigation pane, expand **System Center Configuration Manager -> Site Database > Computer Management -> Collections**.
2. Right-click on **All Systems** and select **Out of Band Management -> Discover Management Controllers**.
3. Right-click on **Collections** and select **New > Collection** from the menu.
4. In the General screen of the New Collections Wizard, enter a name for your collection (in the document example we use "Intel AMT KVM Capable Systems").
5. Click **Next**.
6. Click on the **Query Rules Property** button. The button icon is a yellow data base as shown in Figure 3.



**Figure 3: Query Rules Property Button**

7. In the Query Rules Properties dialog, enter a name for the Query. In the example we use Intel AMT Version 6.
8. In the Resource Class drop down menu, select **System Resource** (default).
9. Click **Edit Query Statement**.
10. Select the Criteria tab.
11. Click the **New Criteria** button as shown in Figure 4 below.



**Figure 4: New Criteria Button**

12. In the Criterion Properties dialog, select **Simple Value** from the Criterion Type drop-down menu.
13. Click **Select** and enter the following information:
  - Attribute Class = **AMT Agent**
  - Attribute = **AMT**
14. Click **OK**.

15. For the **Operator** field, select **is greater than or equal to** from the drop-down menu.
16. Enter **6.0.0** for the **Value** field and click **OK**.
17. An Integrated Intel Graphics adapter is required for KVM Remote Control. Click the **New Criteria** button.
18. In the Criterion Properties dialog, select **Simple Value** from the Criterion Type drop-down menu.
19. Click **Select** and enter the following information:
  - Attribute Class = **Video Controller**
  - Attribute = **Adapter Compatibility**
20. Click **OK**.
21. For the **Operator** field, select **is like** from the drop-down menu. Enter **Intel Corporation** for the **Value** field and click **OK**.
22. In the Query Statement Properties dialog, click **OK**.
23. In the Query Rules Properties dialog, click **OK**.
24. In the Membership Rules screen, click **Next**.
25. In the Advertisements screen, click **Next**.
26. In the Security screen, click **Next**.
27. In the Confirmation screen, click **Close**.
28. In the left-hand pane of the ConfigMgr Console, right-click on your new collection (**Intel AMT KVM Capable Systems** in the document example) and select **Update Collection Membership** from the menu.
29. Click **OK** in the warning dialog.
30. Right-click the new collection and choose **Properties**.
31. The Collection ID is displayed near the bottom. Write this value down.

## 3.3 Alternative Configurations

This section presents some alternatives to the method described in section 3.1.

### 3.3.1 Specify the Admin Credentials

Setting “use currently logged in credentials” has the disadvantage that the automation service used in section 3.2 must have admin rights to Intel AMT. If this is not desired, you may set this to “no” and then specify the Admin User Name and Password. The UCRD document *Extra Configuration for Intel AMT Using Microsoft ConfigMgr* (<http://communities.intel.com/docs/DOC-5215>) has information on using this configuration.



#### NOTE

*The password is stored in **clear text** inside setting.bat. As such, it is recommended that settings.bat and/or kvm.bat be modified to encrypt the password. This is not covered by this document. An alternative is to be extremely careful with where the file is stored, so that only trusted users can access it. Use this method at your own risk.*

### 3.3.2 Using a standard VNC viewer

It is possible to use a standard VNC viewer such as Real VNC's Free Viewer in place of Real VNC Viewer Plus. To do this, you must set a valid RFB Password and set "Enable KVM Only" to "no". This will cause Intel AMT to listen for connections from a standard VNC viewer on port 5900. When connecting, use the RFB Password to authenticate. Note, this configuration is less secure than the one outlined in section 3.1 of this document. For more information on this type of configuration see section 7 of the UCRD document *Out of Box Configuration for KVM Remote Control* (<http://communities.intel.com/docs/DOC-4795>). For steps on using Real VNC's Free Viewer see section 6 of the UCRD document *Out of Box Configuration for KVM Remote Control* (<http://communities.intel.com/docs/DOC-4795>).

### 3.3.3 Disable User Consent

It is possible to disable user consent as part of the initial configuration. To do this, run **OptinOff.bat** (should already be in **c:\kvm** as part of the previously downloaded UCRD *Out-of-Box Configuration for KVM Remote Control*) after running **KVMon.bat**. Then, in VNC Viewer Plus set User Consent off as shown below.

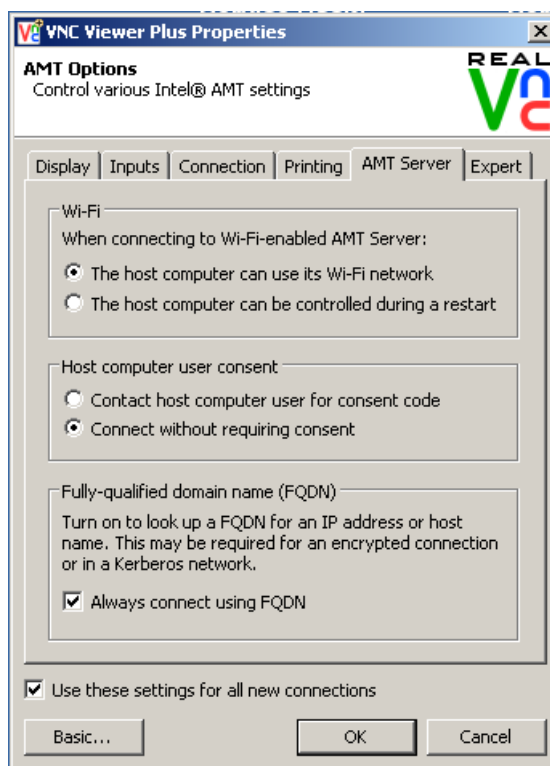


Figure 5: Setting User Consent to Off in VNC Viewer Plus

## 4 Using RealVNC VNC\* Viewer Plus

---

This section outlines the basic steps to connect with RealVNC VNC Viewer Plus. For more information on VNC Viewer Plus see the following:

- RealVNC's Documentation:  
<http://www.realvnc.com/products/viewerplus/1.1/win.html>
- Help Desk Console for Non-TLS Environments, describes using RealVNC Viewer Plus in a Digest, non-TLS environment with emphasis on help desk tasks. These task apply here as well: <http://communities.intel.com/docs/DOC-4910>

### 4.1 Configuring Viewer Plus

Follow the steps below:

1. Click **Start -> Programs -> RealVNC -> VNC Viewer Plus**.
2. Click **Options**.
3. Click **Advanced**.
4. Click the **Connection Tab**.
5. Ensure **Use single sign-on if VNC Server supports it** is selected. This will enable VNC Viewer Plus to use Kerberos credentials. Note that VNC Viewer Plus only allows use of the currently logged on user. You should not be prompted for a user name / password.
6. Click the **AMT Server** tab.
7. Ensure that **Always connect using FQDN** is selected. This will cause VNC Viewer Plus to translate IP addresses to FQDNs as needed for TLS and Kerberos.
8. *Only require if using a Help Desk level user account:* Ensure the Host computer user consent option matches the current setting in Intel AMT. If you followed steps in section 3.1 of this document, set this option to **Contact host Computer for User Consent**.
9. Click **OK**.

### 4.2 Establishing a KVM Remote Control Session

Follow the steps below:

1. Click **Start -> Programs -> RealVNC -> VNC Viewer Plus**.
2. On the New Connection screen, set the following (the order is important):
  - For **Connection Mode** select **Intel AMT KVM**.
  - For **AMT Server** enter the FQDN of the remote PC.
  - For **Encryption** select **TLS**.
3. Click **Connect**.

4. You should not be prompted for Intel AMT credentials. If you are, Kerberos login has failed. Ensure you are logged in as a user with permissions to Intel AMT. You may also try logging out and back in to get a new Kerberos token.
5. Click **OK**.
6. The KVM Remote Control session starts. Depending on how KVM Remote Control was configured you will either be prompted for user consent or be at the remote client's desktop. If the latter, you are done with these steps. Proceed to the conclusion paragraphs after these steps.
  - For more details on User Consent, refer to the UCRD document *Quick KVM Remote Control for Brand New 2010 Intel® Core™ vPro™ Processor Based PCs*, section 6, available at the link below.  
<http://communities.intel.com/docs/DOC-4795>
7. On the Managed Client screen a sprite is displayed with a consent code. Enter this code into the viewer window on the console. **Note:** Do not use the number pad. Once the code is entered you will have remote keyboard, video, and mouse control of the remote client.

Congratulations, you are ready to use KVM Remote Control with your Intel AMT enabled systems that were configured with Microsoft ConfigMgr. For information and ideas on what to do with a KVM Remote Control session, see section 4 of the UCRD document *Help Desk Console for Non-TLS Environments*, available at:

<http://communities.intel.com/docs/DOC-4910>